

the information is for statistical purposes only.

NOTE: No one may use any part of the record to decide on individuals' rights, benefits, or entitlements. You must release records in a format that makes it impossible to identify the real subjects.

(d) The Archivist of the United States and the National Archives and Records Administration (NARA) to evaluate records for permanent retention. Records stored in Federal Records Centers remain under Air Force control.

(e) A federal, state, or local agency (other than the Department of Defense) for civil or criminal law enforcement. The head of the agency or a designee must send a written request to the system manager specifying the record or part needed and the law enforcement purpose. The system manager may also disclose a record to a law enforcement agency if the agency suspects a criminal violation. This disclosure is a Routine Use for all Air Force systems of records and is published in the FEDERAL REGISTER.

(f) An individual or agency that needs the information for compelling health or safety reasons. The affected individual need not be the record subject.

(g) The Congress, a congressional committee, or a subcommittee, for matters within their jurisdictions.

(h) A congressional office acting for the record subject. A published, blanket Routine Use permits this disclosure. If the material for release is sensitive, get a release statement.

(i) The Comptroller General or an authorized representative of the General Accounting Office on business.

(j) A court order of a court of competent jurisdiction, signed by a judge.

(k) A consumer credit agency according to the Debt Collections Act when a published system notice lists this disclosure as a Routine Use.

(l) A contractor operating a system of records under an Air Force contract. Records maintained by the contractor for the management of contractor employees are not subject to the Privacy Act.

§ 806b.35 Disclosing the medical records of minors.

Air Force personnel may disclose the medical records of minors to their parents or legal guardians. The laws of each state define the age of majority.

(a) The Air Force must obey state laws protecting medical records of drug or alcohol abuse treatment, abortion, and birth control. If you manage medical records, learn the local laws and coordinate proposed local policies with the servicing SJA.

(b) Outside the United States (overseas), the age of majority is 18. Unless parents or guardians have a court order granting access or the minor's written consent, they will not have access to minor's medical records overseas when the minor sought or consented to treatment between the ages of 15 and 17 in a program where regulation or statute provides confidentiality of records and he or she asked for confidentiality.

§ 806b.36 Disclosure accountings.

System managers must keep an accurate record of all disclosures made from any system of records except disclosures to DoD personnel for official use or disclosures under the FOIA. System managers may use AF Form 771, 'Accounting of Disclosures'.

(a) System managers may file the accounting record any way they want as long as they give it to the subject on request, send corrected or disputed information to previous record recipients, explain any disclosures, and provide an audit trail for reviews. Include in each accounting:

- (1) Release date.
- (2) Description of information.
- (3) Reason for release.
- (4) Name and address of recipient.

(b) Some exempt systems let you withhold the accounting record from the subject.

(c) You may withhold information about disclosure accountings for law enforcement purposes at the law enforcement agency's request.

§ 806b.37 Computer matching.

Computer matching programs electronically compare records from two or more automated systems which may include the Department of Defense, another federal agency, or a state or

§ 806b.38

other local government. A system manager proposing a match that could result in an adverse action against a federal employee must meet these requirements of the Privacy Act:

(a) Prepare a written agreement between participants.

(1) Secure approval of the Defense Data Integrity Board.

(2) Publish a matching notice in the FEDERAL REGISTER before matching begins.

(3) Ensure full investigation and due process.

(4) Act on the information, as necessary.

(b) The Privacy Act applies to matching programs that use records from:

(1) Federal personnel or payroll systems.

(2) Federal benefit programs where matching:

(i) Determines federal benefit eligibility,

(ii) Checks on compliance with benefit program requirements,

(iii) Recovers improper payments or delinquent debts from current or former beneficiaries.

(c) Matches used for statistics, pilot programs, law enforcement, tax administration, routine administration, background checks and foreign counterintelligence, and internal matching that won't cause any adverse action are exempt from Privacy Act matching requirements.

(d) Any activity that expects to participate in a matching program must contact SAF/AAIA immediately. System managers must prepare a notice for publication in the FEDERAL REGISTER with a Routine Use that allows disclosing the information for use in a matching program. Send the proposed system notice to SAF/AAIA. Allow 180 days for processing requests for a new matching program.

(e) Record subjects must receive prior notice of a match. The best way to do this is to include notice in the Privacy Act Statement on forms used in applying for benefits. Coordinate computer matching statements on forms with SAF/AAIA through the MAJCOM Privacy Act Officer.

32 CFR Ch. VII (7-1-98 Edition)

Subpart J—Training

§ 806b.38 Who needs training.

The Privacy Act requires training for all persons involved in the design, development, operation and maintenance of any system of records. Some persons may need more specialized training. They include information managers, supervisors, and individuals working with medical, financial, security, and personnel records.

§ 806b.39 Training tools.

Helpful aids include:

(a) AFH 37-146⁵, 'Privacy Act Training', a self-paced course.

(b) 'The Privacy Act of 1974,' a 32-minute film developed by the Defense Privacy Office. Consult your local audiovisual library.

(c) 'A Manager's Overview, What You Need to Know About the Privacy Act'. Contact SAF/AAIA for copies.

NOTE: Formal school training groups that develop or modify blocks of instruction must send the material to SAF/AAIA for coordination.

Subpart K—Privacy Act Reporting

§ 806b.40 Privacy Act Report (RCS: DD-DA&M(A)1379).

By March 1, of each year, MAJCOM and FOA Privacy Act officers must send SAF/AAIA a report covering the previous calendar year. The report includes:

(a) Total number of requests granted in whole.

(b) Total number of requests granted in part.

(c) Total number of requests denied and the Privacy Act exemptions used.

(d) Total number of requests for which no record was found.

(e) Total number of amendment requests granted in whole.

(f) Total number of amendment requests granted in part.

(g) Total number of amendment requests wholly denied.

(h) Specific recommendations for changes to the Act or the Privacy Act Program.

⁵See footnote 1 to section 806b.11, of this part.